ты обеспечивается применением мер правового, организационного, сыскного, криминалистического характера.

Создание такой системы защиты на практике связано с решением широкого и разнопланового набора проблем. В их числе задачи разработки стратегии и тактики обеспечения безопасности банка; структурирование и уточнение целей и задач обеспечения безопасности; разработка комплекса основных мер, направленных на достижение указанных целей; подготовка предложений по совершенствованию правового, нормативно-методического, научно-технического и организационного обеспечения безопасности [5].

Список литературы

1. ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». М. : Стандартинформ, 2009.

2. ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», М. : Стандартинформ, 2011.

3. Стандарт Банка России СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

4. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2–2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».

5. ISO/IEC27035:2011 «Information Technology. Security Techniques. Information Security Incident Management».

УДК 004.056.53

А. А. Бабкина
Научный руководитель: канд. пед. наук, доц. О. Р. Уторов
Южно-Уральский государственный университет, Челябинск

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ «ОПЛАТЕ В ОДНО КАСАНИЕ»

Аннотация. В статье рассматриваются актуальные угрозы информационной безопасности при предоставлении банками функций безналичного расчета так называемого «в одно касание» без ввода ПИН-кода с помощью мобильного телефона в приложениях «AndroidPay», «ApplePay», «SamsungPay» и др. Раскрывается один

из способов мошенничества в безналичном расчете денежных средств с помощью специального устройства скиммера.

Ключевые слова: Информационная безопасность; защита информации; безналичный расчет; банковская карта; скиммер; AndroidPay; ApplePay.

В настоящее время, в период развития технологий, когда с каждым днем, часом, минутой великие умы человечества ведут исследования делают опыты и создают будущее, важной особенностью является огромное желание многих людей заработать. При этом для некоторых их них ответ на вопрос: «Заработать как: честно или нет?» не имеет значения, главное — это деньги. А в условиях развития информационных технологий информация как ни что иное выступает в роли денег. Это может быть абсолютно любая информация в разных масштабах, как глобальных, так и локальных.

Рассмотрим один из примеров. Гражданин заполняет анкету, указывая свой адрес, телефон, фамилию, имя, отчество или даже паспортные данные и номер СНИЛСа. На первый взгляд, в принципе ничего особенного, ведь это простая формальность, но, если будут нарушены требования защиты информации, и эти данные попадут в руки мошенника, который захочет обогатиться за ваш счет, это будет не так сложно. Но еще проще не искать данные в анкетах, а просто считать их специальным устройством, например так называемым скиммером с банкомата, и забрать деньги.

Скиммер — это специальное миниатюрное считывающее информацию переносное устройство, которое различными способами незаконно устанавливается к банкомату. Такие приспособления по сути своей являются несанкционированным доступом к защищаемой конфиденциальной информации клиента и помогают мошенникам получить (своровать) данные банковских карт, в частности ее реквизиты, ПИН-код и т. д., — другими словами, всю информацию, записанную на магнитной полосе. Скиммер может быть представлен в форме пластиковой накладки, прикрепляемой к кардридеру, и незаметной пользователю видеокамерой в держателе для рекламы рядом с банкоматом. Также распространены скимеры в виде специальных накладок на клавиатуру, считывающих порядок набора ПИН-кода. Устанавливаться и крепиться к банкоматам скиммеры могут с помощью обычного двустороннего скотча или застежки-«липучки». Например, если клавиатура была вогнутой, то специальная накладка сделает панель более плоской.

Но на сегодняшний день крупные банки, разрабатывая новые правила к защите информации, с учетом вновь выявленных актуальных угроз информационной безопасности, влекущих значительный ущерб как для клиентов, так и для самого банка, научились противостоять такого рода мошенникам. Такие

банки стали оборудовать банкоматы камерами, специальными экранами, информация с которых видна только пользователю перед ним и не видна посторонним лицам, находящимся в непосредственной близости, считыватель карт имеет неправильную округлую или изогнутую форму, которая затрудняет или даже делает невозможной установку специальных устройств, предназначенных для негласного получения информации.

Но развитие информационных технологий не стоит на месте, и в настоящее время стала популярна одна из функций безналичного расчета так называемого «в одно касание» с помощью мобильного телефона в приложениях «AndroidPay», «ApplePay», «SamsungPay» и др. С точки зрения информационной безопасности и безопасности денежных средств в целом, это означает, что теперь украсть деньги мошенникам стало еще проще. Если клиент банка может расплачиваться картой, не вводя ПИН-код, или просто подносить телефон, то почему то же самое не может сделать злоумышленник, только с инициативой со своей стороны? Все знают, что кассовый аппарат может быть беспроводным, а значит, его можно убрать во вместительный карман, за пазуху или в сумку, настроить на считывание и просто сесть рядом в общественном транспорте, встать рядом в очереди или просто подойти спросить время. Одно мгновение — и деньги уже на счету у другого человека. Причем при этом не надо сообщать никаких данных о себе, своей карте и другой информации.

Еще одной существенной угрозой информационной безопасности будет являться потеря телефона или карты с этой подключенной функцией. Ведь пока не заблокируется карта, любой человек может совершать покупки, пока не закончатся деньги или минусовой баланс не достигнет своего лимита, а возвращать потраченные средства банка придется клиенту, а не мошеннику.

Вместе с тем, если у карты нет функции оплаты без ввода ПИН-кода, то, даже зная секретный CVV2/CVC2 код (трехзначный код на обороте карты), злоумышленник не сможет совершить операцию перевода, т.к. обычно требуется SMS-подтверждение с привязанного к карте номера.

Таким образом, следует констатирвать, что с каждым днем злоумышленники придумывают различные способы и средства для того, чтобы украсть как можно больше и как можно проще денежных средств клиентов банка, именно поэтому, по нашему мнению, действующая на сегодняшний день в банках система защиты информации при предоставлении функции оплаты «в одно касание», т. е. без ввода ПИН-кода, пока еще требует своего совершенствования.